REMARKS

The Examiner has rejected Claims 1-9 and 12-35 under 35 U.S.C. 101 as being directed towards non-statutory subject matter. Specifically, the Examiner has argued that "Claims 1, 20 and 30 are directed toward an intrusion detection system" and that "[t]he claimed steps do not result in a tangible result." Applicant respectfully disagrees and asserts that, in fact, independent Claim 1 claims a "computer-implemented method," and independent Claim 30 claims a "computer program product embodied on a computer readable medium," as claimed.

Applicant further emphasizes that independent Claims 1 and 20 recite "generating classification rules" and "select[ing] an action to be performed on said classified packets" (emphasis added - see this or similar, but not necessarily identical language in the aforementioned independent claims). Clearly, applicant's independent Claims 1 and 20 produce a tangible result, such as, for example, generated classification rules and a selected action to be performed, in the context claimed by applicant. Additionally, in Claim 20, applicant claims "select[ing] an action to be performed on said classified packets" (emphasis added), as claimed. Applicant respectfully asserts that selecting an action to be performed, as claimed, provides a tangible result.

The Examiner has rejected Claims 1, 3-9, 13-19, 30, and 31-35 under 35 U.S.C. 103(a) as being unpatentable over Vaidya (U.S. Patent No. 6,279,113 B1), in view of McRae (U.S. Patent No. 6,970,462 B1). Further, the Examiner has rejected Claims 20-29 under 35 U.S.C 103(a) as being unpatentable over Copeland, III (U.S. Publication No. 2002/0144156 A1), in view of McRae (U.S. Patent No. 6,970,462 B1). Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of at least a portion of dependent Claims 31 and 32.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the Vaidya and McRae references, the Examiner has argued that "it would have been obvious...to employ the teachings of McRae within the system of Vaidya in order to enhance the performance and efficiency of the system." Applicant disagrees and respectfully asserts that it would not have been obvious to combine the teachings of the Vaidya and McRae references, especially in view of the vast evidence to the contrary.

For example, Vaidya relates to an intrusion detection system that utilizes attack signature profiles, while McRae relates to classifying packets based on an access control list. To simply glean features from a classification system that utilizes an access control list, such as that of McRae, and combine the same with the *non-analogous art* of an intrusion detection system that utilizes attack signature profiles, such as that of Vaidya, would simply be improper. Attack signature profiles "are each descriptive of identifiable characteristics associated with particular network intrusion attempts" (Vaidya-Col. 3, lines 12-16), whereas in access control lists, access to specific source and/or destination addresses are denied (McRae-Col. 6, lines 12-18). "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed.

Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992) In view of the vastly different types of problems an intrusion detection system which utilizes attack signature profiles addresses as opposed to a classification system which utilizes an access control list, the Examiner's proposed combination is inappropriate.

Moreover, applicant respectfully asserts that the McRae reference even *teaches away* from applicant's specific claim language. In particular, McRae relates to classifying packets based on an access control list, where such access control list controls access (by allowing or denying access) to specific source and/or destination addresses (McRae-Col. 6, lines 12-18). Applicant, however, claims "signature profiles identifying patterns associated with network intrusions" and "comparing said classified packets to at least a subset of the signature profiles" (see the independent claims-emphasis added). Clearly, using an access control list, as in McRae, *teaches away* from using signature profiles, as applicant claims. Applicant respectfully points out that a *prima facie* case of obviousness may also be rebutted by showing that the art, in any material respect, teaches away from the claimed invention. *In re Geisler*, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed. Cir. 1997).

Thus, applicant respectfully asserts that the first element of the *prima facie* case of obviousness has not been met, as noted above. More importantly, applicant also respectfully asserts that the third element of the *prima facie* case of obviousness has not been met by the prior art reference excerpts relied on by the Examiner.

For example, with respect to independent Claims 1 and 30, the Examiner has relied on Col. 5, lines 24-59; and Col. 8, line 62 – Col. 9, line 6 from McRae to make a prior art showing of applicant's claimed technique "wherein the classification is carried out by a first classification stage capable of classifying the data packets based on a first set of packet characteristics, and a second classification stage capable of classifying the data packets received from the first classification stage based on a second set of characteristics" (see this or similar, but not necessarily identical language in the aforementioned independent claims).

Applicant respectfully asserts that the excerpts from McRae relied on by the Examiner merely teach that "the packet header involved in the packet classification is divided into sections (fields) such as 16 bit portions" and that "[o]nce, this is performed, a data lookup table is built for each of the packet header fields" (Col. 5, lines 27-30). Additionally, the excerpts teach that "the created data lookup tables, typically, one for each packet header field, is merged two at a time to form intermediate second level data lookup tables, if any" (Col. 5, lines 32-35) and that "[t]he second level data lookup tables are then merged two at a time to form intermediate third level lookup tables" (Col. 5, lines 37-39). Further, McRae teaches that "[t]he merging proceeds until one final data lookup table is formed" (Col. 5, lines 39-40) and "[t]he results in the final data lookup table represent all the possible packets to be classified" (Col. 5, lines 44-46).

However, simply disclosing that "[t]he merging [of data tables] proceeds until one final data lookup table is formed" and that "[t]he results in the final data lookup table represent all the possible packets to be classified" (emphasis added), as in McRae, fails to even suggest a technique "wherein the classification is carried out by a first classification stage capable of classifying the data packets **based on a first set of packet characteristics**, and a second classification stage capable of classifying the data packets received from the first classification stage **based on a second set of characteristics**" (emphasis added), as claimed by applicant. Clearly, McRae teaches using such final data lookup table to classify packets, which does not specifically relate to the classification process itself, and therefore cannot meet applicant's claimed technique by which "the classification is carried out," as claimed by applicant.

Additionally, the excerpts from McRae relied on by the Examiner also teach that "each packet header entry has a bitmap representing the filtering rules that matches this entry" and that "[t]he bitmap can be used to selectively provide a desired result of the classification" (Col. 5, lines 46-49). Further, in Col. 8, lines 62-66, McRae teaches that "[the] final equivalence set provides all the theoretical possible combinations of rules given any packet header values, and for any of these possible outcomes, there is a bitmap

indicating which rules are matching" and that "[b]y doing a find-first-set on the bitmap, the first matching rule can be obtained."

However, disclosing that "each packet header entry has a bitmap representing the filtering rules that matches this entry" and that "[t]he bitmap can be used to selectively provide a desired result of the classification" (emphasis added), as in McRae, fails to even suggest "a first classification stage capable of classifying the data packets **based on a first set of packet characteristics**, and a second classification stage capable of classifying the data packets received from the first classification stage **based on a second set of characteristics**" (emphasis added), as claimed by applicant. Applicant emphasizes that McRae simply fails to even suggest "a first classification stage...and a second classification stage," not to mention that the "first classification stage [is] capable of classifying the data packets **based on a first set of packet characteristics**" and that the "second classification stage [is] capable of classifying the data packets received from the first classification stage **based on a second set of characteristics**" (emphasis added), as claimed by applicant.

Still yet, it seems the Examiner has also relied on Official Notice in rejecting applicant's above emphasized claim language by stating that "classification of data packets with multi-level stages is well known in the art, which has the advantage of enhancing the performance efficiency of the system." The Examiner has further relied on McRae as an example to support such rejection, however, as noted above, McRae fails to disclose applicant's specifically claimed technique. Even assuming *arguendo* that the Examiner's assertion is correct, applicant respectfully points out that merely alleging that "classification of data packets with multi-level stages is well known in the art," as alleged by the Examiner, fails to rise to the level of specificity of applicant's claim language, namely "a first classification stage capable of classifying the data packets based on a first set of packet characteristics, and a second classification stage capable of classifying the data packets received from the first classification stage based on a second set of characteristics" (emphasis added), as claimed.

Thus, applicant formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

> "If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

With respect to independent Claim 20, the Examiner has relied on paragraphs 0157 - 0159 and 0163 - 0165 from the Copeland reference, in addition to Col. 5, lines 24-59 and Col. 8, line 62 - Col. 9, line 6 in McRae to make a prior art showing of applicant's claimed "detection engine operable to perform a table lookup at the flow table to select an action to be performed on said classified packets based on the classification, wherein comparing said classified packets to at least a subset of the signature profiles is one of the actions."

Applicant respectfully asserts that the excerpts from Copeland relied on by the Examiner merely disclose that "the flow collector thread...searches linearly through the entire flow data structure ... to find flows that have been inactive for a certain time period" after which "a logic tree analysis is done to classify [the inactive flows] as either a normal flow, or a potential probe or other suspicious activity" (paragraph 0157 – emphasis added). Further, the excerpts teach that "[t]he packet classifier thread 610 collects information on network operations such as packets and bytes" and that "[t]he alert manager thread 630 writes the updated data to various output files for use by the user interface" (paragraph 0165 – emphasis added).

However, merely teaching the classification of inactive flows and the writing of updated data to output files, as in Copeland, fails to teach "a detection engine operable to perform a table lookup at the flow table to select an action to be performed on said classified packets based on the classification" and does not even suggest "comparing said **classified** packets to at least a subset of the signature profiles" (emphasis added), as claimed by applicant. Applicant respectfully asserts that simply nowhere in the excerpts relied on by the Examiner is there any teaching or suggestion of "select[ing] an action to

be performed on said classified packets based on the classification [and] comparing said classified packets to at least a subset of the signature profiles," as applicant claims.

Furthermore, the excerpts from McRae relied on by the Examiner simply relate to "the creation of data tables for header values that match against a set of classification rules" (Col. 5, lines 24-26), and "provid[ing] all the theoretical possible combinations of rules given any packet header values…[such] that there is a bitmap indicating which rules are matching" (Col. 8, lines 62-65). Applicant respectfully asserts that simply teaching identifying classification rules that match header values, as in McRae, fails to even suggest any sort of "action to be performed on said classified packets," in addition to a "compari[son of] said classified packets to at least a subset of the signature profiles," as applicant claims.

Additionally, with respect to independent Claim 20, the Examiner has relied on Col. 5, lines 24-59; and Col. 8, line 62 - Col. 9, line 6 from McRae to make a prior art showing of applicant's claimed "signature classifier comprising a first stage classifier operable to classify packets according to at least one packet field into groups and a second stage classifier operable to classify said packets within each of the groups according to packet type or size."

Applicant respectfully asserts that the excerpts relied upon by the Examiner generally teach "an exemplary procedure that allows for the creation of data tables for header values that match against a set of classification rules" (Col. 5, lines 24-26) and that "[t]he results in the final data lookup table represent all the possible packets to be classified." However, the excerpts relied upon by the examiner fail to even suggest "a signature classifier comprising a **first stage classifier** operable to classify packets according to at least one packet field into groups and a **second stage classifier** operable to classify said packets within each of the groups according to packet type or size" (emphasis added), as claimed by applicant. Clearly, McRae teaches using such final data lookup table to classify packets, which does not specifically relate to the classification process itself, and therefore cannot meet applicant's claimed "**first stage classifier**

operable to classify packets according to at least one packet field into groups and a **second stage classifier** operable to classify said packets within each of the groups according to packet type or size" (emphasis added), as claimed by applicant.

Additionally, the excerpts from McRae relied on by the Examiner teach that "each packet header entry has a bitmap representing the filtering rules that matches this entry" and that "[t]he bitmap can be used to selectively provide a desired result of the classification" (Col. 5, lines 46-49). Further, in Col. 8, lines 62-66, McRae teaches that "[the] final equivalence set provides all the theoretical possible combinations of rules given any packet header values, and for any of these possible outcomes, there is a bitmap indicating which rules are matching" and that "[b]y doing a find-first-set on the bitmap, the first matching rule can be obtained."

However, disclosing that "each packet header entry has a bitmap representing the filtering rules that matches this entry" and that "[t]he bitmap can be used to selectively provide a desired result of the classification" (emphasis added), as in McRae, fails to even suggest "a **first stage classifier** operable to classify packets according to at least one packet field into groups and a **second stage classifier** operable to classify said packets within each of the groups according to packet type or size" (emphasis added), as claimed by applicant.

Still yet, it seems the Examiner has also relied on Official Notice in rejecting applicant's above emphasized claim language by stating that "classification of data packets with multi-level stages is well known in the art, which has the advantage of enhancing the performance efficiency of the system." The Examiner has further relied on McRae as an example to support such rejection, however, as noted above, McRae fails to disclose applicant's specifically claimed technique. In addition, applicant respectfully points out that merely alleging that "classification of data packets with multi-level stages is well known in the art," as alleged by the Examiner, fails to rise to the level of specificity of applicant's claim language, namely "a first stage classifier operable to classify packets according to at least one packet field into groups and a second stage

classifier operable to classify said packets within each of the groups according to packet type or size" (emphasis added), as claimed.

Applicant again formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP cited above.

To this end, applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, and the prior art reference excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has at least substantially incorporated at least a portion of the subject matter of former dependent Claims 31 and 32 into the independent claims.

With respect to the subject matter of former Claim 31 (now at least substantially incorporated into the independent claims), the Examiner has relied on Col. 5, lines 24-59 from McRae to make a prior art showing of applicant's claimed technique "wherein the first set of packet characteristics includes at least one of a destination address, a protocol type, and a destination port number" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully asserts that the excerpt relied upon by the Examiner merely teaches "an exemplary procedure that allows for the creation of data tables for header values that match against a set of classification rules" (Col. 5, lines 24-26) and that "the packet header involved in the packet classification is divided into sections (fields) such as 16 bit portions" (Col. 5, lines 27-29 – emphasis added). Additionally, McRae teaches that "[t]he results in the final data lookup table represent all the possible packets to be classified" (Col. 5, lines 44-46). However, McRae fails to specifically suggest any of a "destination address, a protocol type, and a destination port number" (emphasis added), in the context claimed by applicant. Clearly, dividing a packet header into sections, such

as 16 bit portions, as in McRae, fails to even suggest "classifying the data packets based on...at least one of a destination address, a protocol type, and a destination port number" (see the same or similar, but not necessarily identical language in the independent claims-emphasis added), as specifically claimed by applicant.

Additionally, with respect to the subject matter of former Claim 32 (now at least substantially incorporated into the independent Claims 1 and 30, and at least substantially previously included in Claim 20), the Examiner has relied on the following excerpt from McRae to make a prior art showing of applicant's claimed technique "wherein the second set of packet characteristics includes at least one of a packet type and a size" (see this or similar, but not necessarily identical language in the aforementioned independent claims).

> "An action of matching a packet against a database of rules (or rulesets) can be implemented as a memory lookup. For instance, if a packet header has a total of 114 bits (each Internet Protocol (IP) address: 32 bits, each layer 4 (L4) port number: 16 bits, 8 bit protocol, 8 bit type of service (TOS)/Precedence, flags: 2 bits), the 114 bits could be used as an entry to a memory bank such as a CAM to classify the incoming packets. While this guarantees that every incoming packet would be classified, the memory size involved would make the implementation impractical.
>
> An observation is made that the rules themselves need not treat the packet header as one single header, but instead, each packet header field could be treated separately. For example, each rule can separately specify values for IP source and destination addresses, IP protocol and etc. Some fields may have implicit dependence, such as when L4 port numbers are specified, the IP protocol may need to be specified as either a Transmission Control Protocol (TCP) or a User Datagram Protocol (UDP). In instances where each rule makes no reference to a particular field, such as a 32 bit IP source address, an assumption can be made that all values of this field will match (i.e., a wildcard). A wildcard IP address can be simply treated as a value of zeros and a mask of zeros." (Col. 3, line 60 - Col. 4, line 15 - emphasis added)

Applicant respectfully asserts that the excerpt relied upon by the Examiner merely teaches that "[a]n action of matching a packet against a database of rules (or rulesets) can be implemented as a memory lookup" where "each packet header field could be treated separately." Further, McRae teaches that "each rule can separately specify values for IP source and destination addresses, IP protocol and etc." However, simply disclosing that

rules can specify source and destination addresses separately, as in McRae, fails to even suggest "at least one of a packet type and a size" (emphasis added), as claimed by applicant. In fact, McRae fails to even suggest "a second classification stage capable of classifying the data packets received from the first classification stage based on [the] second set of characteristics," where "the second set of packet characteristics includes at least one of a packet type and a size" (see Claims 1 and 30-emphasis added), or "a second stage classifier operable to classify said packets within each of the groups according to packet type or size" (see Claim 20-emphasis added), as claimed by applicant.

Again, applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have net been met, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 33, the Examiner has relied on Col. 5, lines 24-59 from McRae to make a prior art showing of applicant's claimed technique "wherein only the second classification stage remains in communication with a flow table for identifying an action to be taken with respect to the data packets."

Applicant respectfully asserts that the excerpt relied upon by the Examiner merely teaches "an exemplary procedure that allows for the creation of data tables for header values that match against a set of classification rules" (Col. 5, lines 24-26) and that "[t]he results in the final data lookup table represent all the possible packets to be classified" (Col. 5, lines 44-46). However, McRae fails to even suggest a technique "wherein only the second classification stage remains in communication with a flow table for identifying an action to be taken with respect to the data packets" (emphasis added), as claimed by applicant. In fact, McRae fails to even suggest "[a] second classification stage," not to mention a technique "wherein **only** the second classification stage remains in communication with a flow table for identifying an action to be taken with respect to the data packets" (emphasis added), as claimed by applicant.

Again, since at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above, a notice of allowance or proper prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new claims 36-37 below, which are added for full consideration:

> "wherein the action includes dropping at least one of the data packets and updating one or more fields in the flow table" (see Claim 36); and
>
> "wherein the packet type is determined based on a TCP flag" (see Claim 37).

Again, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested. Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P318).

Respectfully submitted,
Zilka-Kotab, PC.

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100